The Impact of the European Data Protection Reform on Citizens. Which Choices Remain?*

Janneke Slöetjes**

목 차

Ⅰ. Introduction

European laws that protect the personal data and privacy of citizens have always ranked amongst the highest developed data protection laws in the world. In January 2012, the European Commission (EC) has launched a reform of these rules, introducing a draft Data Protection Regulation (the 'Draft Regulation) which has channelled a very fierce debate about the future of data protection and privacy. The draft tries to accommodate new

* This paper aims to provide you with an outline of European data protection law and the changes presented in the Draft Regulations. This paper will firstly explore the current rules in short and comment on the background of the current law and the need for new legislation. Secondly, it will describe the most interesting features of the new Draft Regulation. Finally, the paper will describe the political state of play: which forces influence the reform and what are possible outcomes?

** Lawyer

technologies and provide security and choice for both citizens and businesses - but will it do what it promises?

The reform of the European Framework attracts a lot of attention, not only within Europe, but from all over the world. The European debate is likely to shape future data protection law on a very big scale, as many countries aim to achieve maximum interoperability with the European framework. Also, many laws throughout the world are based on the European standards, so it can be expected that new European changes will lead to changes to for instance Latin-American data protection laws.

Ⅱ. The current European data protection framework

European data protection laws were harmonized for the first time in 1998, when the European Data Protection Directive (95/46/EC, hereinafter referred to as 'the Directive')[1] was implemented in the laws of the European Member States. Prior to this Directive, each European Member States had its own data protection law. The Directive is built upon the 1980 OECD Guidelines and consists of data protection principles regarding transparency, legitimate purpose and proportionality. These principles can also be found in South-Korea's PIPA law of 2011.

1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

1. The current framework is based upon the following principles.

1.1 Information and access(articles 10, 11, 12)

The data subject has the right to be informed when his personal data is being processed. The party responsible for the processing(data controller) must provide its name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair. The data subject also has the right to access all data processed about him, as well as a right to demand rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules. (art. 12)

1.2 Legal basis (article 7)

Data processing should always be based on one out of six legal grounds. Data can be processed when

- consent has been obtained; or
- processing is necessary for the performance of or the entering into a contract; or
- processing is necessary for compliance with a legal obligation; or
- processing is necessary in order to protect vital interests of the data subject; or
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests

are overridden by the interests for fundamental rights and freedoms of the data subject.

1.3 Legitimate purpose (art. 6 b)

Personal data may only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes.

1.4 Proportionality (article 6)

Personal data may be processed only insofar the data is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data must furthermore be accurate and up to date and should not be kept in a form which permits identification of data subjects for longer than necessary.

1.5 Sensitive data (article 8)

When sensitive personal data, such as religious beliefs, political opinions, health, sexual orientation, race, or trade union membership, are being processed, stricter rules apply.

1.6 Right to object (article 14)

The data subject may object at any time to the processing of personal data for the purpose of direct marketing.

1.7 Automated decision making (article 15)

Decisions which produce legal effects or significantly affect a data subject may not be based solely on automated processing of data. A form of appeal should be provided when automatic decision making processes are used.

Ⅲ. The need for new legislation : what is lacking in Europe?

1. Technological changes

The changes proposed by the European Commission are heavily influenced by technological changes. The rise in electronic processing, the growth of online services and the fact that the amount of personal data is and will continue to rise strongly has obviously inspired a great number of the proposed changes to the law. The European Commission strives to protect personal data better in an online environment and to give citizens more control over their data.

2. Economic growth in Europe

The European Commission wants to streamline the laws for the private sector in order to make it easier for companies to do business in Europe. Replacing 27 different data protection laws with one Regulation makes it easier for businesses to comply. Also, certain administrative requirements, such as notifying processing operations to Data Protection Authorities (hereinafter also referred to as DPA's) will be abolished.

3. Enforcement and sanctions

Enforcement of data protection laws throughout Europe has never been consistently strong. Some Data Protection Authorities are relatively powerful and strong, while others are severely understaffed. Understaffed DPA's cannot enforce data protection law adequately. Another issue related to enforcement is that the maximum sanctions are very low in some Member States. For example, the maximum sanction for a breach of certain administrative requirements related to data protection in the Netherlands is EUR 4,500 (6.500.000 South-Korean Won). DPA's do have the power to investigate companies or governmental organizations which are suspected to breach of data protection law. When establishing such a breach, a DPA may impose a high penalty during the period the breach is not remedied. However, such a regime is only successful when DPA's have sufficient time to investigate more than a handful of cases per year.

4. Open norms

Finally, the abovementioned data protection principles are mainly open norms. This makes them flexible and allows them to apply in a multitude of situations and across both the private and the public sector. On the other hands, the openness causes vagueness and uncertainty. Also, many terms have been interpreted somewhat differently across Member States. The European legislator has trusted these open norms to be filled in by case law. However, there have not been many court cases on data protection related issues. Court cases relating to privacy and data protection are often handled based on articles 7 and 8 of the European Charter of Human rights

or article 8 of the European Convention of Human Rights. These articles protect the private lives of individuals as well as the right of protection of personal data. For the most part, companies confronted with data protection requirements have a hard time to figure out what exactly open norms such as 'adequacy' or 'legitimate interest' mean in practice. The European Commission tries to fill in more details in the current law, clarifying some legal concepts.

Ⅳ. Changes proposed by the Draft Regulation

The European Commission has put forward a proposal[2] for new data protection rules in January 2012, announcing an update to the data protection framework. Firstly, it wants to change the legal structure of the law from a Directive to a Regulation. A regulation will be directly applicable and enforceable in all European Member States, which means the law will be exactly the same throughout Europe. This is advantage for businesses, as they no longer will have to comply with a patchwork of different rules.

Secondly, the European Commission has proposed a number of interesting updates to the existing regime. These updates are intended to decrease the number of administrative sanctions for data controllers (companies as well as governmental organizations that process personal data) as well as to provide more control and transparency to data subjects (the citizens whose personal data are being processed).

---

2) 25 January 2012, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data(General Data Protection Regulation), (COD) 2012/0011.

1. What's in it for citizens?

Hereinafter is an overview of the most interesting new provisions in the Draft Regulation that are intended to award citizens better protection of their personal data.

1.1 A better definition of protected data (article 4(1) Draft Regulation)

The European Commission proposes a small change to the definition of 'personal data' by clearly stating that online identifiers such as device numbers, IP addresses or cookie identifiers can identify a natural person. As such, such data fall under the scope of the Draft Regulation and are protected.

1.2 Stricter rules for consent (article 7 Draft Regulation)

The European Commission proposes to change the consent requirement from regular consent to 'explicit consent'. This means that when a data controller wants to obtain consent from a citizen, it has to ask explicitly whether a person consents to the use of its personal data for a specific purpose. This is specifically intended to give citizens more control over their data and to prevent situations where consent is 'hidden' in general terms and conditions.

Secondly, it means that consent cannot be considered obtained validly when there is a significant imbalance between the data controller requesting the consent and the data subject (citizen). A doctor can therefore not base processing of personal data on consent, and neither can an employer. Such parties need to find another legal ground as the basis for data processing.

1.3 A right to be forgotten (article 17 Draft Regulation)

One of the most controversial additions to the Draft regulation is the so-called “right to be forgotten”. This is in the first place due to the quite controversial title: contrary to what it claims, it does not imply a full right for citizens to have their data erased under all circumstances. The provision is however quite badly drafted and as a result hard to understand. This has raised severe worries about the exact scope of the provision, and led to a debate regarding possible infringments of the right to free speech.[3)]

The European Commission has proposed that every citizen has the right to obtain from the controller the abstention from further dissemination of its personal data. In addition, when a data controller has made personal data public, it should take all reasonable steps to inform third parties who are processing the data, that the citizen has requested the erasure of the information, of links to the information of of copies of the personal data.

There are a number of exceptions to this right, for instance when retention of the data is necessary for exercising the right to free speech, for public health reasons or for statistical, historical or scientific research purposes. Nevertheless, it is feared that the right to be forgotten in the from proposed by the European Commission will put too much pressure on data controllers to erase data they published and to have it erased by third parties as well.

1.4 The right to take your data with you (data portability, article 18 Draft Regulation)

The European Commission introduces an addition to the right to access,

3) See for instance 〈http://techliberation.com/2010/11/05/the-conflict-between-a-right-to-be-forgotten-speech-press-freedoms/〉 for an overview of objections raised against the so-called ‘right to be forgotten’.

erase and correct personal data. Under the draft Regulation, it becomes possible for data subjects to obtain an electronic copy of their personal data, so that they can take their data from one data controller to another if they wish. This new provision is intended to prevent lock-in of customers in for instance social networks. It can however also be of use for other services, as it allows you for instance to port your telecom data to another provider and receive a good new offer based on your exact use, or to track the energy consumption in your household by obtaining an overview that can be analyzed. The big advantage over a mere copy is that it is a digital file, which allows you to analyze the data yourself or upload it to another company of your choice. Next to preventing lock-in, this provision aims to increase competition between services in Europe, as it becomes easier for citizens to move from one service to another when they are dissatisfied.

1.5 New rules prohibiting profiling (article 20 Draft Regulation)

The current article 15 of the Directive prohibits automated decision making unless a number of criteria are met. For one, automated decisions may not be based solely on sensitive data. There should also be additional safeguards in place, such as information regarding the fact that automated decisionmaking (profiling) takes place and the consequences of such profiling.

1.6 Data breaches must be reported to DPA's and citizens (article 31 and 32 Draft Regulation)

The Draft Regulation contains provisions that require data controllers to report data breaches to DPA's as soon as possible (generally within 24

hours). When the breach is likely to affect citizens adversely, the breach must also be reported to them.

1.7 A new regime for compliance and higher penalties (article 79 Draft Regulation)

Under the new proposal, Data Protection Authorities from European countries will work closer together in order to bridge the differences between the different authorities. Decisions taken by one of the authorities will be submitted to other authorities as well in order to guarantee consistent enforcement throughout the EU.

Secondly, all DPA's will be granted the same enforcement power, including powerful sanction possibilities. A breach of data protection rules may lead to a fine of 0,5% up to 2% of the company's worldwide global turnover.

Ⅴ. Political state of play

Since the proposal was put forward by the European Commission, both the Council (of Ministers; formed by the Ministers of Justice from each Member State) as well as the European Parliament ("EP") have provided comments and amendments to the draft proposal. The negotiations that take place within the Council are secret, only the outcomes of each round of negotiations are being published. The deliberations of the European Parliament are more public and open. As such, the European Parliament is the place sought out by lobbyists to influence the proposal and convince the Members of European Parliaments (MEPs) to file amendments to alter

the proposed Regulation.

1. The Brussels lobbystorm

The influence of lobbyists on this particular piece of draft legislation has proven to be very strong. The responsible Commissioner, Ms. Viviane Reding, has declared the lobby around data protection the 'fiercest lobby ever'.[4)]

Internet and IT companies, both American and European, lobby very hard for more flexibility and less rules, as do telecom operators, banks, (online) advertisers, publishing houses and insurers. As a result of heavy lobbying, an astounding total of 4000 amendments has been filed over the course of a little over a year. Research by Austrian activists[5)] has shown that many MEPs copypasted proposals directly from business lobby briefs. Especially politicians of the conservative European People's Party have used this method to file their amendments to the proposal. Most amendments aim to provide businesses with more flexibility around data processing and greater freedom to store, analyze, use and combine personal data of citizens.

European activists of digital civil rights have of course also lobbied the Parliament but have been outnumbered for the most.

2. European Parliament voting results

Even though the European Parliament has not yet conducted its plenary vote on this issue, there have been three votes in opinion Committees[6)]

---

4) 〈http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html〉

5) See www.lobbyplag.eu for an overview of all amendments and which politicians copypasted most.

in the Parliament. The outcome of such opinion votes is a good predictor for what will happen during a plenary vote. It shows clearly that all Committees have favored the interests of businesses over the interests and rights of citizens. This has resulted in changes to many of the proposals that were newly launched by the European Commission. Consent no longer needs to be explicit, data portability should be limited, data breach notification is only necessary in severe cases and the rules to subject people to profiling will become more lenient. Sanctions are being slashed, and MEPs have introduced a special sub-category of personal data (so-called 'pseudonymous data', were a direct identifier is replaced by a pseudonym) that requires less protection, giving companies more freedom to use such data, especially online. Many MEPs also support more flexible rules to export data to third countries, regardless of the level of protection of personal data in these countries, and less strict purpose limitation principles.

3. Next steps

From a civil society point of view, the voting results so far have been very discouraging. Next up will be the vote in the LIBE (Civil Liberties, Justice and Home Affairs) Committee, which is the leading Committee on this file. As such, the responsible Member of Parliament who is also a member of LIBE, will take all results from the previous voting rounds into account and present a full draft package before the vote which is scheduled for 21 October 2013.

---

6) The involved Opinion Committees are: Internal Market and Consumer Protection(IMCO), Industry, Research and Energy(ITRE) and Legal Affairs (JURI).

Given the previous outcome, such a package cannot contain many positive solutions. However, not only the Parliament, but also the European Commission as well as the Council each have an equal stake in the negotiations before settling on a final text, which then will have to be approved by a majority of the MEPs in a plenary voting session. It seems unlikely that the European Commission will agree to an extremely watered down version of its original proposal.

Ⅵ. Conclusion: what remains for citizens?

Although it is a bit too early to be totally discouraged, it is very well possible that European citizens will end up with worse data protection law and less protection of privacy than they currently enjoy under the Directive. The European Commission has tried to bring matters forward and modernize data protection law, but its efforts are currently being met with counterproposals that aim to achieve the exact opposite.

This is a rather ironic situation since everyone is well aware that personal data of citizens is very valuable and will continue to play a growing role in our economy and society. Sadly, politicians seem to perceive it not as a fundamental right that deserves protection, but merely as currency for the digital economy.

(투고일 2013년 12월 20일, 심사(의뢰)일 2014년 1월 16일, 게재확정일 2014년 2월 21일)

Key Words : data protection, privacy, personal data, European legislation, digital rights, digital economy

[국문초록]

유럽 개인정보보호 개정이 시민에게 미치는 영향
-어떤 선택을 할 것인가-

Janneke Slöetjes*

시민들의 개인 데이터와 프라이버시를 보호하는 유럽 법률은 전 세계적으로 최고 수준의 데이터 보호 법률이라는 위치를 차지하고 있다. 2012년 1월 유럽연합집행위원회(EC)는 이러한 법규 개혁을 개시해 데이터 보호 및 프라이버시의 미래에 대한 격렬한 논쟁을 완화시킨 데이터 보호 규정안(Draft Regulation)을 도입했다. 이 안은 새로운 기술을 도입하려 하고 있으며, 시민 개인과 사업체 둘 모두에 보안 및 선택 기회를 제공하고 있다. 그러나 그것으로 약속한 것을 성취해낼 수 있을까?

유럽집행위원회는 기존 법규에 여러 새로운 개념을 도입했다. 이는 사업비용을 경감하고 시민 개인이 자신의 개인 데이터를 사용하는데 있어 더 많은 통제력을 발휘할 수 있게 하기 위한 것이었다. 변경 내용으로는 온라인 환경에서 데이터를 더 잘 보호하기 위한 목적의 개인 데이터를 더 잘 정의하는 것, 동의를 얻는 것에 관한 좀 더 엄격한 규정과 소위 망각할 권리 등이 포함되어 있는데, 이러한 변경내용은 시민들로 하여금 자신에 관해 공개된 정보를 삭제할 수 있게 해준다. 이러한 새로운 권리는 언론의 자유를 보호하는 것에 관해 의문을 제기하고 있다. 뿐만 아니라 제안내용에는 시민들이 자신의 데이터 전체 사본을 얻을

* 변호사

수 있는 권리와 데이터 침해 통지 규정과 데이터 보호 법률을 위반한 기업이나 정부에 대해 더 높은 수준의 제재 조치 등이 포함되어 있다.

유럽 의회는 이 입법안에 대해 수많은 반대 제안에 직면해오고 있다. 이러한 제안들 중 대부분은 사업체가 자신들의 이익을 위해 시민 데이터를 처리할 수 있는 여지를 더 많이 제공하기 위한 목적을 지니고 있기 때문에 프라이버시 보호를 축소시키는 결과를 낳게 될 것이다. 이는 의회 의원들이 도입한 상당수의 제안과 수정안이 로비스트들의 제안에서 비롯된 것이기 때문에 그리 놀랄 일도 아니다.

따라서 이 입법 과정이 어떻게 결말을 맺을지는 매우 불확실하다. 유럽인들은 현재 수준 보다 자신들의 개인 데이터 보호 수준이 축소되는 것으로 결말을 맺을 수도 있다.

본 논문은 데이터 보호법의 업데이트 필요성을 분석하고, 유럽집행위원회가 제안한 새로운 추가 사항을 탐색해볼 것이다. 마지막으로 본 논문은 정치적 활동 상태와 가능한 결과에 대한 설명을 제시할 것이다.

주제어 : 데이터 보호, 개인 정보 보호, 개인정보, 유럽의 법률, 디지털 저작권, 디지털 경제